UNITED STATES DISTRICT COURT
DISTRICT OF MAINE

IN THE MATTER OF THE SEARCH OF	)	
74 GEORGE STREET, SOUTH	)	
PORTLAND, ME 04106, MORE	)	Case No. 2:23-mj-00120
PARTICULARLY DESCRIBED	)	
IN ATTACHMENT A	)	Filed Under Seal

AFFIDAVIT IN SUPPORT OF AN APPLICATION FOR A WARRANT TO SEARCH AND SEIZE

I, Sean R. Cohen, being first duly sworn, hereby depose and state as follows:

Introduction and Agent Background

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a warrant to search the residence of Wainette Woodbine ("WOODBINE"), located at 74 George Street, South Portland, ME 04106 ("TARGET RESIDENCE"), further described in Attachment A, for the things described in Attachment B, which includes electronic devices such as WOODBINE's cellular telephone. As set forth below, I submit that probable cause exists that WOODBINE has committed violations of Title 18, United States Code, Section 1344 (bank fraud).

2. I am a Special Agent with the U.S. Department of Homeland Security (DHS), Homeland Security Investigations (HSI), and have been so employed since December of 2011. I have a Master of Arts degree in Leadership Studies from the University of Texas at El Paso and have successfully completed the Criminal Investigator Training Program and Special Agent Training at the Federal Law Enforcement Training Center in Glynco, Georgia. Among my responsibilities as a Special Agent is the investigation of financial crimes. I have received training in the area of financial crimes and am experienced in having conducted multiple investigations involving financial crimes and financial scams.

3. This affidavit is intended to show only that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

Probable Cause

Origins of Investigation

4. Throughout the course of this investigation, agents have learned that a victim with the initials J.A. and who is a resident of West Palm Beach, Florida is the suspected victim of a lottery winnings scam. The overall monetary amount sent by J.A. to the suspected scammers is estimated at over $400,000.00. West Palm Beach Police Department Detective and Homeland Security Investigations (HSI) Task Force Officer (TFO) Fernando Palacios interviewed J.A. and G.B. (J.A.'s live-in girlfriend) on Wednesday, July 28, 2021. J.A. stated he has mailed over $400,000.00 as requested by "David Brooks" and "John Hawkins." Brooks and Hawkins are believed to be fake names used by the people instructing J.A. to send money. During a follow-up interview with J.A. and G.B. on Thursday, February 3, 2022, J.A. said that Hawkins told J.A. that J.A. would be receiving 44 million dollars from Winners International, a group that had communicated with Publishers Clearing House (PCH). Throughout the course of the investigation, investigators learned that Brooks and Hawkins contacted J.A. through phone calls and emails.

5. During an interview with J.A. and G.B. on Thursday, February 3, 2022, J.A. said Hawkins told J.A. that Winners International, the organization J.A. believed he had won money from, has communicated with PCH and that J.A. would be receiving $44 million. Also during the interview with J.A., J.A. gave me and TFO Palacios a printout of emails J.A. received from Hawkins and allegedly from PCH. J.A.'s email address of johnw1934@me.com received an email from email address winnerspch2018@gmail.com on Saturday, December 18, 2021 with the subject stating in the email Subject Line, "CONGRATULATIONS ON YOUR PRIZE

WINNINGS". The email stated that J.A. was required to follow Mr. John Hawkins' instructions to ensure that J.A.'s "prize winnings are delivered safely." The printout showed that this email to J.A. from winnerspch2018@gmail.com was then forwarded to email address jh9456528@gmail.com by email address winnerspch2018@gmail.com.

6. Investigators have warned J.A. numerous times over the past several months that he is the victim of a scam and he should stop sending money relating to this scam. J.A.'s girlfriend G.B. who lives with him has also warned him that he is a victim of a scam. Despite these warnings, J.A. continues to communicate with the scammers.

Woodbine Identified

7. G.B. later provided information indicating J.A. sent $10,000.00 in September 2022 to Wainette WOODBINE. At that time, driver license checks showed that WOODBINE had a registered address of 750 Sanford Rd. Unit 8, Wells, ME 04090. However, United States Postal Service records show that WOODBINE requested a change of address from the old address of 750 Sanford Rd. Unit H8, Wells, ME, to the new address of 74 George St, South Portland, ME 04106-6328 (TARGET RESIDENCE) as of November 8, 2022. Immigration checks showed that WOODBINE was born in Jamaica and is a Legal Permanent Resident in the U.S.

Bank and Phone Records

8. In January 2023, Kennebunk Savings Bank provided records pertaining to bank accounts owned by WOODBINE and her mother, Marsha Chung. Kennebunk Savings Bank account x5555 is owned by WOODBINE and is a checking account that was opened on May 3, 2022. Kennebunk Savings Bank account x3677 is owned by both WOODBINE and Chung and is a savings account that was opened on April 19, 2022. WOODBINE's Kennebunk Savings Bank account profile information includes home and cellphone numbers of 207-251-6644 and email

address wainettewoodbine@gmail.com. Chung's Kennebunk Savings Bank account profile information includes a home phone number of 239-687-8124 and email address morrismarsha17@yahoo.com.

9. Records show that victim J.A. wired $10,000.00 to WOODBINE's x5555 savings account on September 21, 2022, and an additional $10,000.00 on September 27, 2022 to the same account. After the two wires for $10,000.00 each were completed, money was then transferred to WOODBINE's and Chung's Kennebunk Savings Bank savings account x3677. Also, money was transferred to various subjects via Zelle transactions. Additionally, a wire for $1,000.00 and a wire for $2,300.00 were sent on September 23, 2022, and September 28, 2022, respectively, from WOODBINE's and Chung's x3677 account to "Ssali Juma" in Uganda.

10. In February 2023, AT&T provided the following subscriber information for AT&T user Wainette WOODBINE:

- Financial Liable Party
    - Name: Wainette Woodbine
    - Credit Address: 750 Sanford Rd APT Unit 8, Wells, ME 04090
    - Customer Since: 12/16/2021
    - Contact Home Phone: (207) 251-6644
    - Contact Work Phone: (111) 111-0002
    - Contact Home Email: wainettewoodbine@gmail.com
- User Information
    - MSISDN: (207) 251-6644
    - Name: Wainette Woodbine
    - User Address: 750 Sanford Rd, Wells, ME 04090

- Service Start Date: 10/01/2021
- Contact Home Email: morrismarsha17@yahoo.com (this email address is the same email address associated to Marsha Chung's AT&T profile with phone number 239-687-8124.

11. AT&T provided the following subscriber information for AT&T user Marsha Morris WOODBINE (AKA Marsha CHUNG.):

- Financial Liable Party
  - Name: Marsha Morris Woodbine
  - Credit Address: 750 Sanford Rd Unit 8, Wells, ME 04090
  - Customer Since: 06/12/2014
  - Contact Home Phone: (239) 687-8124
  - Contact Work Phone: (239) 687-8124
  - Contact Home Email: morrismarsha17@yahoo.com
- User Information
  - MSISDN: (239) 687-8124
  - MSISDN Active: 06/12/2014 – Current
  - Name: Marsha Chung
  - User Address: 83 Bypass Rd, Wells, ME 04090
  - Service Start Date: 06/12/2014
  - Contact Home Email: marsha@yahoo.com

12. In December 2022, Western Union provided subpoena returns indicating Wainette WOODBINE sent $450.00 on February 19, 2022 via Western Union to a person in Gauteng, South Africa. WOODBINE's phone number listed for the transaction is 207-251-6644, the same phone

number associated to WOODBINE's Kennebunk Savings Bank and AT&T user profiles.

13. Kennebunk Savings Bank provided surveillance videos for various bank actions and transactions conducted by WOODBINE. One video Kennebunk Savings Bank provided is entitled "Opening checking 5/3" and is the surveillance video for the account opening of account x5555. The video is approximately 21 minutes and 16 seconds long and shows a woman who appears to be WOODBINE sitting in an office with a bank representative. Another video Kennebunk Savings Bank provided is entitled "opening savings 4/19" and is the surveillance video for the account opening of account x3677. The video is approximately 19 minutes and 47 seconds long and shows a bank representative, a woman who appears to be WOODBINE, and another subject wearing a facemask. Both WOODBINE and the subject wearing a facemask can be seen filling out paperwork and handing the bank representative cards that appear to be identification. The subject wearing a mask is likely Chung since Chung is the co-owner of the account.

14. Kennebunk Savings Bank provided a video entitled "wire 9/23" that coincides with the outgoing wire sent to "Ssali Juma" in Uganda on September 23, 2022. The wire was for $1,000.00 and was sent from WOODBINE and Chung's x3677 account. The video entitled "wire 9/23" is approximately 8 minutes and 9 seconds long and shows a woman who appears to be WOODBINE. In the video, WOODBINE is sitting in an office at Kennebunk Savings Bank with a bank representative. WOODBINE has a cell phone with her and periodically scrolls through it. According to the video time stamp, at approximately 9:27 a.m. WOODBINE shows the bank teller her cellphone.

15. Kennebunk Savings Bank provided a video entitled "wire 9/28" that coincides with the outgoing wire sent to "Ssali Juma" in Uganda on September 28, 2022. The wire was for the amount of $2,300.00 and was sent from WOODBINE and Chung's x3677 account. The video

entitled "wire 9/28" is approximately 15 minutes and 1 second long and shows a woman who appears to be WOODBINE. In the video, WOODBINE walks into and sits in an office with a bank representative. WOODBINE has a cellphone with her. At approximately 8:38 a.m., WOODBINE holds the cellphone to her ear as if to make a phone call or listen to a message. At approximately 8:39 a.m., WOODBINE takes the cellphone from her ear and begins to scroll through the cellphone. At approximately 8:51 a.m., WOODBINE holds her cellphone towards the bank representative as if to show the bank representative something from the phone's screen. WOODBINE stops showing her cellphone to the bank representative at approximately 8:52 a.m. WOODBINE then holds her cellphone to her ear as if to make a phone call or listen to a message.

16. Kennebunk Savings Bank provided a video entitled "deposit 5/13" that is approximately 1 minute and 12 seconds long. The video shows a woman who appears to be WOODBINE driving up to a bank ATM in a silver Infiniti SUV and then conducting a transaction at the ATM. A 2007 silver Infiniti FX35 with Maine license plate 1455ZK is registered to Wainette WOODBINE, and the residence information for the vehicle registration is 74 George Street, South Portland, ME 04106 (TARGET RESIDENCE). The vehicle registration has an effective date of 11/02/2022 and an expiration of 11/30/2023. A 1995 blue Toyota Corolla with Maine license plate 3604ZE is also registered to WOODBINE at the 74 George Street address.

17. AT&T provided call detail records pertaining to WOODBINE's phone number 207-251-6644, which showed that this number sent and received several voice calls and text messages to and from Jamaican phone numbers beginning with the phone prefix 876 between June 11, 2022 and January 2, 2023. Moreover, on September 22, 2022 and September 24, 2022—shortly after the September 21, 2022 wire from J.A. to WOODBINE's account—there were incoming and outgoing text messages and voice calls between WOODBINE's 6644 phone number

and Jamaican phone numbers beginning with the phone prefix 876.

18. Zelle records show that WOODBINE has an active profile status pertaining to Kennebunk Savings Bank, and the recipient token associated to the account is email address wainettewoodbine@gmail.com. According to Zelle, a token is the email or U.S. mobile phone number used to identify an enrolled user and associates that user with the enrolled account. Zelle records show that WOODBINE has another active profile account with Town & Country Federal Credit Union, and the recipient token for the account is WOODBINE's phone number, 207-251-6644.

19. Zelle information provided by Early Warning Services lists various transactions conducted in WOODBINE's accounts. After $10,000.00 was deposited into WOODBINE's x5555 account on September 21, 2022 from J.A., money was transferred from the x5555 account via Zelle to the following subjects on the listed dates:

$400.00 (Recipient: Nashemma Thomas) (Posted date: 9/22/2022)

$600.00 (Recipient: Marsha Chung) (Posted date: 9/22/2022)

$1,000.00 (Recipient: Tameka Lawrence-Stewart) (Posted date: 9/22/2022)

$534.00 (Recipient: Nashemma Thomas) (Posted date: 9/26/2022)

20. Zelle's token information for Nashemma Thomas listed the email address nashemma@stu.ncu.edu.jm. United States Immigration records indicate that Nashemma Thomas has an email address of nashemma@stu.ncu.edu.jm, is a Jamaican citizen, and recently traveled from Jamaica to Atlanta on May 19, 2022.

21. A police report from Watertown, CT Police Department, dated December 21, 2022, indicated that elderly scam victims J.C. and G.C. are victims of a PCH scam, similar to the one in this case. J.C. stated she received a call in November 2022 from someone saying they were from

PCH and that J.C. and G.C. won the sweepstakes. J.C. said she received an email later outlining her prize as $12.5 million and two Mercedes Benz vehicles. J.C. ended up paying requested fees to different people, including $25,000.00 for a "Federal Approval Stamp" and then another $25,000.00 for a "Customer Approval Stamp." J.C. stated she continued to receive phone calls from individuals claiming to be from PCH who instructed her to send multiple checks to different individuals and different addresses. J.C. was told the people she was sending money to are attorneys. J.C. said she sent out approximately fifteen checks in increments of $20,000.00, $25,000.00, or $30,000.00 over the course of about a month around November-December 2022, totaling around $500,000.00. J.C. said she realized her accounts were frozen at the bank, that the bank flagged the activity in her accounts, and that is when J.C. and G.C. realized they were being scammed.

22. The Watertown, CT Police Department provided information indicating that J.C. and G.C. mailed a check from their Thomaston Savings Bank account in the amount of $25,000.00 to Chantika Hesloph with a payee address of 74 George Street, South Portland, Maine (TARGET RESIDENCE) which had a FedEx tracking number. FedEx information indicates this package was delivered on December 6, 2022. The check was cashed in December 2022. J.C. and G.C. mailed another check from their Thomaston Savings Bank account. This check was also in the amount of $25,000.00, was again paid to Chantika Hesloph, and was sent to the TARGET RESIDENCE via FedEx. FedEx information indicates this packaged was delivered on December 3, 2022. This check was also cashed. Driver license information indicates Chantika Vevien Hesloph-Thomas has a Maine driver's license and a registered address at 74 George St, South Portland, ME 04106 (TARGET RESIDENCE). Immigration information indicates Hesloph-Thomas is a citizen of Jamaica.

23. AT&T records for WOODBINE's phone number 207-251-6644 show multiple incoming and outgoing voice calls between WOODBINE's phone number and the phone number associated with Hesloph-Thomas's Zelle account, 207-423-1482. There were incoming and outgoing calls between both phone numbers from June 2022 through January 2023, indicating continuous and recurrent contact. In addition to the calls between WOODBINE's and Hesloph-Thomas's phone numbers, Zelle information indicates both WOODBINE and Hesloph-Thomas have transferred money to each other between April 2022 and July 2022 via Zelle. Zelle information reveals one transaction in which WOODBINE transferred Hesloph-Thomas $495.00 on 7/17/2022 via Zelle, and the "Payment Memo" for the transaction was "Rent for 3 months".

24. On Wednesday, March 29, 2023, Watertown, CT Police Department informed me that the scam victim, J.C., called the Watertown detective and left a voicemail, saying that "James Walker" called her today. J.C. recognized "Mr. Walker's" voice as being part of the scam in which J.C. is a victim, and J.C. remembered "Mr. Walker" used that name a long time ago in the scam. "Mr. Walker" said he is from FBI New Haven and that they have her money. "Mr. Walker" provided the phone number 203-408-7606. I attempted to call the 7606 number on Wednesday, March 29, 2023. No one answered the call, and I heard a voicemail message saying the 7606 phone number subscriber is a "TextNow" subscriber.[1] From my training and experience, scammers will often use phone and device applications like TextNow, so that the scammers can call and send messages more discreetly and make it appear that the scammers are using a local

[1] Based on my training and experience and from open source research, TextNow is a phone application that provides "a VoIP (Voice over Internet Protocol) service that allows users to text and call any number in Canada & the USA. Additionally, users are able to purchase credits to make international long-distance calls. TextNow provides the user with a real phone number which can be used on any smartphone, tablet, or desktop computer with an Internet connection. The application can be used on multiple devices under the same login at the same time." https://help.textnow.com/hc/en-us/articles/360052815553-What-is-TextNow-

number that matches the victim's area code.

25. On Wednesday, March 22, 2023, an HSI Special Agent in Portland, ME conducted surveillance at the TARGET RESIDENCE. There were multiple vehicles parked at the residence including the silver 2007 Infiniti SUV with Maine tag 1455ZK that is registered to WOODBINE, which was parked in the driveway.

TECHNICAL TERMS

26. Based on my training and experience, I use the following technical terms to convey the following meanings:

a. IP Address: The Internet Protocol address (or simply "IP address") is a unique numeric address used by computers on the Internet. An IP address looks like a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.

b. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

c. Storage medium: A storage medium is any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

COMPUTERS, ELECTRONIC STORAGE, AND FORENSIC ANALYSIS

27. As described above and in Attachment B, this application seeks permission to search for records that might be found on the TARGET RESIDENCE, in whatever form they are found. One form in which the records might be found is data stored on a computer's hard drive or other storage media. Thus, the warrant applied for would authorize the seizure of electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

28. *Probable Cause.* I submit that if a computer or storage medium is found on the TARGET RESIDENCE, there is probable cause to believe those records will be stored on that computer or storage medium, for at least the following reasons:

a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used

by an active file—for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

c. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

29. *Forensic Evidence.* As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the crime described on the warrant, but also for forensic electronic evidence that establishes how computers were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on any storage medium in the TARGET RESIDENCE because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that

show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.

b. As explained herein, information stored within a computer and other electronic storage media may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within a computer or storage media (e.g., registry information, communications, images and movies, transactional information, records of session times and durations, internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the computer or storage media. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculpating or exculpating the computer owner. Further, computer and storage media activity can indicate how and when the computer or storage media was accessed or used. For example, as described herein, computers typically

contain information that log: computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer, and the IP addresses through which the computer accessed networks and the internet. Such information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation. Additionally, some information stored within a computer or electronic storage media may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer may both show a particular location and have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (e.g., a digital camera or cellular phone with an incorporated camera). The geographic and timeline information described herein may either inculpate or exculpate the computer user. Last, information stored within a computer may provide relevant insight into the computer user's state of mind as it relates to the offense under investigation. For example, information within the computer may indicate the owner's motive and intent to commit a crime (e.g., internet searches indicating criminal planning), or consciousness of guilt (e.g., running a "wiping" program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

c. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

30. *Necessity of Seizing or Copying Entire Computers or Storage Media.* In most cases, a thorough search of a premises for information that might be stored on storage media often requires the seizure of the physical storage media and later off-site review consistent with the warrant. In lieu of removing storage media from the premises, it is sometimes possible to make an image copy of storage media. Generally speaking, imaging is the taking of a complete electronic picture of the computer's data, including all hidden sectors and deleted files. Either seizure or

imaging is often necessary to ensure the accuracy and completeness of data recorded on the storage media, and to prevent the loss of the data either from accidental or intentional destruction. This is true because of the following:

a. The time required for an examination. As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how a computer has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on premises could be unreasonable. As explained above, because the warrant calls for forensic electronic evidence, it is exceedingly likely that it will be necessary to thoroughly examine storage media to obtain evidence. Storage media can store a large volume of information. Reviewing that information for things described in the warrant can take weeks or months, depending on the volume of data stored, and would be impractical and invasive to attempt on-site.

b. Technical requirements. Computers can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of computer hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data at the TARGET RESIDENCE. However, taking the storage media off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.

c. Variety of forms of electronic media. Records sought under this warrant could be stored in a variety of storage media formats that may require off-site reviewing with specialized forensic tools.

31. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit seizing, imaging, or otherwise copying storage media that reasonably appear to contain some or all of the evidence described in the warrant, and would authorize a later review of the media or information consistent with the warrant. The later review may require techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

32. Because several people share the TARGET RESIDENCE as a residence, it is possible that the TARGET RESIDENCE will contain storage media that are predominantly used, and perhaps owned, by persons who are not suspected of a crime. If it is nonetheless determined that that it is possible that the things described in this warrant could be found on any of those computers or storage media, the warrant applied for would permit the seizure and review of those items as well.

BIOMETRICS CHARACTERISTICS

33. The warrant I am applying for would permit law enforcement to obtain from certain individuals the display of physical biometric characteristics (such as fingerprint, thumbprint, or facial characteristics) in order to unlock devices subject to search and seizure pursuant to this warrant. I seek this authority based on the following:

a. I know from my training and experience, as well as from information found in publicly available materials published by device manufacturers, that many electronic devices,

particularly newer mobile devices and laptops, offer their users the ability to unlock the device through biometric features in lieu of a numeric or alphanumeric passcode or password. These biometric features include fingerprint scanners and facial recognition features. Some devices offer a combination of these biometric features, and the user of such devices can select which features they would like to utilize.

b. If a device is equipped with a fingerprint scanner, a user may enable the ability to unlock the device through his or her fingerprints. For example, Apple offers a feature called "Touch ID," which allows a user to register up to five fingerprints that can unlock a device. Once a fingerprint is registered, a user can unlock the device by pressing the relevant finger to the device's Touch ID sensor, which is found in the round button (often referred to as the "home" button) located at the bottom center of the front of the device. The fingerprint sensors found on devices produced by other manufacturers have different names but operate similarly to Touch ID.

c. If a device is equipped with a facial recognition feature, a user may enable the ability to unlock the device through his or her face. For example, Apple offers a facial recognition feature called "Face ID." During the Face ID registration process, the user holds the device in front of his or her face. The device's camera then analyzes and records data based on the user's facial characteristics. The device can then be unlocked if the camera detects a face with characteristics that match those of the registered face. Facial recognition features found on devices produced by other manufacturers have different names but operate similarly to Face ID.

d. In my training and experience, users of electronic devices often enable the aforementioned biometric features because they are considered to be a more convenient way to unlock a device than by entering a numeric or alphanumeric passcode or password. Moreover, in some instances, biometric features are considered to be a more secure way to protect a device's

contents. This is particularly true when the users of a device are engaged in criminal activities and thus have a heightened concern about securing the contents of a device.

e. As discussed in this affidavit, based on my training and experience I believe that one or more digital devices will be found during the search. The passcode or password that would unlock the device(s) subject to search under this warrant is not known to law enforcement. Thus, law enforcement personnel may not otherwise be able to access the data contained within the device(s), making the use of biometric features necessary to the execution of the search authorized by this warrant.

f. I also know from my training and experience, as well as from information found in publicly available materials including those published by device manufacturers, that biometric features will not unlock a device in some circumstances even if such features are enabled. This can occur when a device has been restarted, inactive, or has not been unlocked for a certain period of time. For example, Apple devices cannot be unlocked using Touch ID when (1) more than 48 hours has elapsed since the device was last unlocked or (2) when the device has not been unlocked using a fingerprint for 4 hours *and* the passcode or password has not been entered in the last 156 hours. Biometric features from other brands carry similar restrictions. Thus, in the event law enforcement personnel encounter a locked device equipped with biometric features, the opportunity to unlock the device through a biometric feature may exist for only a short time.

g. In my training and experience, the person who is in possession of a device or has the device among his or her belongings at the time the device is found is likely a user of the device. However, in my training and experience, that person may not be the only user of the device whose physical characteristics are among those that will unlock the device via biometric features, and it is also possible that the person in whose possession the device is found is not actually a user

of that device at all. Furthermore, in my training and experience, I know that in some cases it may not be possible to know with certainty who is the user of a given device, such as if the device is found in a common area of a premises without any identifying information on the exterior of the device. Thus, it will likely be necessary for law enforcement to have the ability to require any individual, who is found at the Subject Premises and reasonably believed by law enforcement to be a user of the device, to unlock the device using biometric features in the same manner as discussed above.

h. Due to the foregoing, if law enforcement personnel encounter a device that is subject to search and seizure pursuant to this warrant and may be unlocked using one of the aforementioned biometric features, the warrant I am applying for would permit law enforcement personnel to (1) press or swipe the fingers (including thumbs) of any individual, who is found at the subject premises and reasonably believed by law enforcement to be a user of the device, to the fingerprint scanner of the device; (2) hold the device in front of the face of those same individuals and activate the facial recognition feature, for the purpose of attempting to unlock the device in order to search its contents as authorized by this warrant.

CONCLUSION

34. Based on the foregoing, I submit that this affidavit supports probable cause for a warrant to search the TARGET RESIDENCE described in Attachment A and seize the items described in Attachment B.

Sean Cohen, Special Agent
Homeland Security Investigations

Sworn to telephonically and signed electronically in accordance with the requirements of Rule 4.1 of the Federal Rules of Criminal Procedures

Date: May 04 2023

City and state: Portland, Maine

Judge's signature

Karen Frink Wolf, U.S. Magistrate Judge
Printed name and title